

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

THE CELLULAR DEVICE ASSIGNED IPv6
ADDRESS: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c,
UTILIZED ON 2020-03-02 03:17:29 UTC, WHICH
IS STORED AT PREMISES CONTROLLED BY
T-MOBILE

Case No. 20-MJ-95

APPLICATION FOR A SEARCH WARRANT

I, Clinton Blauser, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 1073 and 2

The application is based on these facts: See Affidavit in Support of Application for Search Warrant.

☒ Delayed notice of 180 days (give exact ending date if more than 30 days: August 30, 2020) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



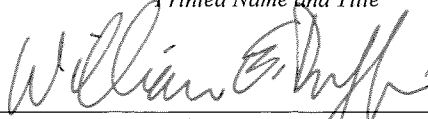
Applicant's signature

Clinton Blauser, Deputy, U.S. Marshal Service

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 3/3/2020



Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge

Printed Name and Title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Clinton Blauser, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned IPv6 address: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c, utilized on 2020-03-02 03:17:29 UTC¹ (the “**TARGET CELL PHONE**”), whose service provider is **T-Mobile**, a wireless telephone service provider headquartered at **4 Sylvan Way Parsippany, NJ 07054**. The **TARGET CELL PHONE** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices (“pen-trap devices”) to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the **TARGET CELL PHONE**.

¹ Coordinated Universal Time (UTC), also referred to as Greenwich Mean Time (GMT), Universal Time (UT), or “Zulu” is an international time scale used in astronomical and aviation publications, weather products, and other documents. UTC uses 24-hour (military) time notation and is based on the local standard time on the 0° longitude meridian which runs through Greenwich, England. Midnight in Greenwich corresponds to 00:00 UTC, noon corresponds to 12:00 UTC, and so on. UTC is six hours ahead of Central Standard Time (CST) and five hours ahead of Central Daylight Time (CDT).

3. I am employed as a Deputy with the United States Marshals Service (USMS) and have held that position for over 9 years. Prior to serving as a Deputy U.S. Marshal, I spent three years working for the Allen County Sheriff's Department in Allen County, Indiana, as a Police Officer and a Confinement Officer. As part of my duties in my current position, I conduct investigations to locate federal and state fugitives. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

4. This affidavit is based upon my personal knowledge, and upon information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. On January 10, 2020, a criminal complaint (case no.: 20-mj-834) and arrest warrant were issued charging **David QUINONES-RIOS** in the Eastern District of Wisconsin and elsewhere with conspiracy to possess with intent to distribute and to distribute controlled substances, in violation of Title 21, United States Code, Section 846; possession with intent to distribute and distribution of controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); attempt to possess with intent to distribute and to distribute controlled substances, in violation of Title 21, United States Code, Section 846; use of communications

facilities to facilitate controlled substance felonies, in violation of Title 21, United States Code, Section 843(b); conspiracy to launder monetary instruments, in violation of Title 18, United States Code, Section 1956(h); and money laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i). On February 11, 2020, a Federal grand jury, sitting in the Eastern District of Wisconsin, returned a forty-four count indictment (case no.: 20-CR-30-JPS), which alleges various violations of Federal law by **QUINONES-RIOS** and twenty-five other co-defendants.

7. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. The United States, including the United States Marshals Service (USMS), is conducting a fugitive investigation of **QUINONES-RIOS** regarding his flight from prosecution, in violation of Title 18, United States Code, Section 1073, for pending Federal charges alleging conspiracy to possess with intent to distribute and to distribute controlled substances, in violation of Title 21, United States Code, Section 846; possession with intent to distribute and distribution of controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); attempt to possess with intent to distribute and to distribute controlled substances, in violation of Title 21, United States Code, Section 846; use of communications facilities to facilitate controlled substance felonies, in violation of Title 21, United States Code, Section 843(b); conspiracy to launder monetary instruments, in violation of Title 18, United States Code, Section 1956(h); and money laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

9. On January 15, 2020, law enforcement officers executed a search warrant in relation to the criminal complaint filed in case no.: 20-mj-834 at a residential property located at GPS coordinates: 18.4068300, -67.173210, in Aguada, Puerto Rico, which had been identified as **QUINONES-RIOS**'s residence. Co-defendants who lived nearby, including David **QUINONES-QUINONES** (**QUINONES-RIOS**'s father), were arrested on January 15, 2020 as well. Since the issuance of **QUINONES-RIOS**'s arrest warrant in this case, **QUINONES-RIOS** has eluded apprehension by law-enforcement authorities and is a fugitive. Given the search of **QUINONES-RIOS**'s residence and the apprehension of nearby coconspirators, there is reason to believe that **QUINONES-RIOS** is aware of his pending Federal charges and has fled in violation of Title 18, United States Code, Section 1073 (Flight to Avoid Prosecution). There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting **QUINONES-RIOS**, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

10. On January 16, 2020, your Affiant conducted a public search of Facebook.com and located the profile user name "Rios Davito" with url: <https://www.facebook.com/davito.rios.56>. Your Affiant confirmed that the account is assigned to **QUINONES-RIOS** based on a comparison between publicly-posted images on the "Rios Davito" Facebook page and photographs of **QUINONES-RIOS** provided to the USMS by the Drug Enforcement Administration (DEA). According to the DEA, **QUINONES-RIOS** uses the alias of "Davito," which is contained within the Facebook account name. Your Affiant was also able to view publicly-posted images on the "Rios Davito" Facebook account timeline. An image date-stamped January 2, 2020 depicted **QUINONES-RIOS** with known co-conspirator Hector Yamil RODRIGUEZ-RODRIGUEZ. On

January 15, 2020, at 1:57 a.m., the user of the “Rios Davito” Facebook account made his last post, which read, “Every day that passes comes out a piggy every day i count with less.”

11. On January 24, 2020, U.S. Magistrate Judge Nancy Joseph signed Pen Register and Trap and Trace orders for the “Rios Davito” Facebook account. On March 1, 2020, Facebook provided your Affiant with the following dates and times when the specified Internet Protocol address (IP address)² accessed the “Rios Davito” Facebook account:

IP Address 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c

Time 2020-03-02 03:17:29 UTC

IP Address 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c

Time 2020-03-02 03:17:28 UTC

IP Address 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c

Time 2020-03-02 03:16:36 UTC

IP Address 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c

Time 2020-03-02 03:13:41 UTC

IP Address 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c

Time 2020-03-02 03:12:27 UTC”

12. Your Affiant utilized the website: www.arin.net (American Registry of Internet Numbers [ARIN]) to obtain the owner and operator of the IPv6 address: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c. According to ARIN, the listed IPv6 is owned and

² An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

operation by **T-Mobile**. Your Affiant has utilized ARIN in the past and knows this website to be reliable. Based on my training and experience, your Affiant believes **QUINONES-RIOS** is using a cellular device (i.e., the **TARGET CELL PHONE**), serviced by **T-Mobile**, to access the “Rios Davito” Facebook account.

13. Based on my training and experience, you Affiant knows that **T-Mobile** is a cellular service provider and does have the ability to connect their cellular service to the internet through Dynamic Internet Protocols. A Dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it's connected to a network. A Dynamic IP address is an automatically configured IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server to every new network node. Dynamic IP addresses are generally implemented by Internet service providers and networks that have a large number of connecting clients or end-nodes. Unlike static IP addresses, Dynamic IP addresses are not permanent. A Dynamic IP is assigned to a node until it's connected to the network; therefore, the same node may have a different IP address every time it reconnects with the network.

14. I know through training and experience, that **T-Mobile** is able to resolve IPv6 addresses. When **T-Mobile** resolves those IP addresses, they are able to identify the user and the specific cellular telephone associated with that user. Providing **T-Mobile** with a IPv6 address and time stamp serves the same function as providing **T-Mobile** with a specific cellular number. Thus, the following IPv6 address and time stamp: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c, utilized on 2020-03-02 03:17:29 UTC, will serve the same function as providing **T-Mobile** the cellular telephone associated with one of its customer accounts.

15. In my training and experience, I have learned that **T-Mobile** is a company that provides cellular telephone access to the general public. I also know that providers of cellular

communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the “sector” (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

16. Based on my training and experience, I know that **T-Mobile** can collect E-911 Phase II data about the location of the **TARGET CELL PHONE**, including by initiating a signal to determine the location of the **TARGET CELL PHONE** assigned IPv6 address: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c, utilized on 2020-03-02 03:17:29 UTC, on **T-Mobile** network or with such other reference points as may be reasonably available.

17. Based on my training and experience, I know that **T-Mobile** can collect cell-site data about the **TARGET CELL PHONE** assigned IPv6 address: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c, utilized on 2020-03-02 03:17:29 UTC. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as **T-Mobile** typically collect and retain cell-site data pertaining to cellular devices to which

they provide service in their normal course of business in order to use this information for various business-related purposes.

18. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data. Based on my training and experience, I know that the Service Provider can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available.

19. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber

Identifier (“IMSI”), or an International Mobile Equipment Identity (“IMEI”). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication’s content.

AUTHORIZATION REQUEST

20. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

21. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

22. I also request that the Court direct **T-Mobile** to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the **T-Mobile**’s services, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on the **T-Mobile**’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate **T-Mobile** for reasonable expenses incurred in furnishing such facilities or assistance.

23. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 180 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of **TARGET**

CELL PHONE would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

24. I further request that the Court direct **T-Mobile** to disclose to the government any information described in Attachment B that is within the possession, custody, or control of **T-Mobile**. I also request that the Court direct **T-Mobile** to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with **T-Mobile** services, including by initiating a signal to determine the location of the Target Cell Phone on **T-Mobile** network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate **T-Mobile** for reasonable expenses incurred in furnishing such facilities or assistance.

25. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the **TARGET CELL PHONE** assigned IPv6: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c, utilized on 2020-03-02 03:17:29 UTC, outside of daytime hours.

ATTACHMENT A
Property to Be Searched

The cellular telephone assigned IPv6 address: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c, utilized on 2020-03-02 03:17:29 UTC (the “**TARGET CELL PHONE**”), whose wireless service provider is T-MOBILE, a company headquartered at 4 Sylvan Way Parsippany, NJ 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of T-Mobile, including any information that has been deleted but is still available to T-Mobile or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), T-MOBILE is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following subscriber and historical information about the customers or subscribers associated with the **TARGET CELL PHONE** for the time period January 15, 2020 through March 3, 2020:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address);
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the **TARGET CELL PHONE**, including:
 - (A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - (B) information regarding the cell tower and antenna face (also known as “sectors” through which the communications were sent and received).
- b. Information associated with each communication to and from the **TARGET CELL PHONE** for a period of 45 days from the date of this warrant, including:
 - i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
 - ii. Source and destination telephone numbers;
 - iii. Date, time, and duration of communication; and
 - iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the **TARGET CELL PHONE** will connect at the beginning and end of each communication.
- c. Information about the location of the **TARGET CELL PHONE** for a period of 30 days, during all times of day and night. “Information about the location of the Subject Phone” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.
 - i. To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of T-MOBILE, T-MOBILE is required to disclose the Location Information to the government. In addition, T-MOBILE must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with T-MOBILE’s services, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on T-MOBILE’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate T-MOBILE for reasonable expenses incurred in furnishing such facilities or assistance.

- ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to Be Seized by the Government

All information described above in Section I that will assist in arresting **David QUINONES-RIOS**, who was charged with violating, *inter alia*, Title 21, United States Code, Section 846, Title 18, United States Code, Section 1956(h) between September 1, 2018 and January 15, 2020, is the subject of an arrest warrant issued on January 10, 2020, and who is suspected to be violating Title 18, United States Code, Section 1073, and is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF
THE CELLULAR DEVICE ASSIGNED IPv6
ADDRESS: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c,
UTILIZED ON 2020-03-02 03:17:29 UTC, WHICH
IS STORED AT PREMISES CONTROLLED BY
T-MOBILE

Case No.: 20.115-95

**APPLICATION FOR ORDER COMMANDING T-MOBILE NOT TO NOTIFY ANY
PERSON OF THE EXISTENCE OF SEARCH WARRANT**

The United States requests that the Court order T-MOBILE, an electronic communications service provider and/or a remote computing service, not to notify any person (including the subscribers or customers of the account(s) listed in the Search Warrant) of the existence of the attached Search Warrant for a time period of six months.

T-MOBILE is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States obtained the attached Search Warrant, which requires T-MOBILE to disclose certain records and information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.*

In this case, such an order would be appropriate because the attached Search Warrant relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation.

Accordingly, there is reason to believe that notification of the existence of the attached Search Warrant will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Some of the evidence in this investigation is stored electronically. If alerted to the investigation, the subjects under investigation could destroy that evidence, including information saved to their personal computers.

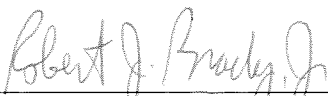
WHEREFORE, the United States respectfully requests that the Court grant the attached Order directing T-MOBILE not to disclose the existence or content of the attached Search Warrant, except that T-MOBILE may disclose the attached Search Warrant to an attorney for T-MOBILE for the purpose of receiving legal advice.

The United States further requests that the Court order that this application and any resulting order be sealed for a time period of six months. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Executed on March 3, 2020, at Milwaukee, Wisconsin.

MATTHEW D. KRUEGER
United States Attorney

By:



ROBERT J. BRADY, JR.
Assistant United States Attorney
United States Attorney's Office, EDWI
517 E. Wisconsin Avenue, Room 530
Milwaukee, Wisconsin 53202
414-297-1724

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF
THE CELLULAR DEVICE ASSIGNED IPv6
ADDRESS: 2607:fb90:0cda:d807:4d1b:b9ae:b4fd:f09c,
UTILIZED ON 2020-03-02 03:17:29 UTC, WHICH
IS STORED AT PREMISES CONTROLLED BY
T-MOBILE

Case No.: 20-MJ-95

**ORDER COMMANDING T-MOBILE NOT TO NOTIFY ANY PERSON OF
THE EXISTENCE OF SEARCH WARRANT**

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding T-MOBILE, an electronic communications service provider and/or a remote computing service, not to notify any person (including the subscribers or customers of the account(s) listed in the Search Warrant) of the existence of the attached Search Warrant for a time period of six months.

The Court determines that there is reason to believe that notification of the existence of the attached Search Warrant will seriously jeopardize the government investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that T-MOBILE shall not disclose the existence of the attached Search Warrant or this Order of the Court, to the listed subscriber or to any other person, for a time period of six months, except that T-MOBILE may disclose the attached Search Warrant and this Order of the Court to an attorney for T-MOBILE for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed for a time period of six months.

3/3/2020
Date

William E. Duffin
WILLIAM E. DUFFIN
United States Magistrate Judge
Case No.: